2018出國差旅報告書

科技部補助國際會議心得報告

參加 Asiacrypt 2018  
(12月3-6 日,澳洲布里斯本)

**報告主筆：楊柏因**

中央研究院資訊科學研究所 研究員

民國107年12月7日

出差期間：107年12月1日至7日

事由： 參加 Asiacrypt 2018 (12月3-6 日,澳洲布里斯本)

感謝： 科技部計畫

共同出差人: 無

出差時間表:

|  |  |
| --- | --- |
| 18/12/1-2 | 由桃園(TPE)搭機抵布里斯本(BNE)，當日參加歡迎晚會 |
| 18/12/3-6 | Asiacrypt 2018 |
| 18/12/6-7 | 由布里斯本(BNE)搭機返台北 |

1. 本次出訪的因緣

本人受邀在此次大會擔任Session Chair。

1. 18/12/3-6 Asiacrypt   
   **本次會議在​​大樓開會。  
     
   主題:** **Dustin Moody 代表美國國家標準局 NIST 發表他們主辦的後量子競賽中的一些官方說法。這是人最多的大會邀請演講。** Moody 表示對第一輪的參賽者，審查的標準主要不是速度而是安全性。他們主要把已破除和有嚴重疑慮的參加者先剔除。另外也把相似同類的演算法盡量擇其優者留下。被破除的和有大問題的有CFPKM, Compact-LWE, DAGS, DME, DRS, GuessAgain, Giophantus, Lepton,McNie, pqsigRM, RaCoSS, RLCE, Walnut-DSA, 已退出的則有 Edon-K, HK17, RankSign, RVB, SRTPI。PQRSA 和 DualModeMS 實在太慢而被剔除 （他很有風度沒有指責 Daniel J. Bernstein 提出 PQRSA 是來搞笑的…筆者註）。他指出凡是相近且 NIST 打算擇優選取一個留下的就會建議他們合併。事實上真的合併的有Round5 = Round2 + Hila5, Rollo = Lake + Locker + Ouroboros-R, NTRU = NTRUEncrypt + NTRU-HRSS-KEM, LEDAcrypt = LEDAkem + LEDApkc，(其中NTRU 和 Round5 才是真的有意義的合併，另兩個只是換湯不換藥…筆者註)。最後競爭最激烈的網格類加密中，留下了 NTRU, NTRU Prime, NewHope, LAC, Round5, Saber, Crystals-Kyber 和 Frodo, 開始前呼聲最高的都留下來了。Moody指出整個比賽有一位大贏家，他一個人參與了第二輪 26 件中共七件的投稿 (筆者按：這是Peter Schwabe 教授，他參與了NewHope, Crystals-Kyber, Crystals-Dilithium, Classic McEliece, MQDSS, SPHINCS+)。 他們有要求第二輪的參賽者把投稿重整，而大部份的參賽者都有交新的程式或修改參數。他們並希望下一輪中大家用 ARM Cortex M4 和 Artix-7的 FPGA來比較演算法在嵌入式系統中的優劣。

**主題:** **本人的演講在第二日早上**。我介紹了多變量密碼學的最近狀況和在 NIST 第二輪中剩下來的參賽者 (Rainbow, LUOV, GeMSS, 和 MQDSS)。

**主題:** 這是一個工作坊。有一半的場次是演講另一半的場次是討論與工作。本人主持其中的一節，除了介紹本人的近作，我也主導討論大家密切討論了關於 Isomorphism of Polynomials 實作一個數位簽名的可能。

**主題:** 主辦單位請到最近很紅的派克特(Chris Peikert)來介紹了網格密碼學的最近狀況包含各類最新的網格類攻擊的現況。他詳述了關於近似網格化約，精確網格化約，篩法和窮舉法等各種攻擊和最新的幾種加密和簽章的方法。  
  
**主題:** 克洛伊。瑪汀黛爾(Chloe Martindale)來介紹了超奇異橢圓曲線同源密碼系統的新一支，即可交換超奇異橢圓曲線同源DH金鑰交換 (CSIDH),這其中的 DH 就表示 Diffie-Hellman, 就是目前最常見的橢圓曲線金鑰交換方式。CSIDH 可以做為DH一個可抽換的取代品 (Drop-In Replacement) 而且其金鑰長和傳輸量都極小，還可沿用很多橢圓曲線的程式碼！其問題是速度很慢且安全性未受考驗。

**主題:** 微軟的科斯特婁 (Craig Costello)前來跟大家報告超奇異橢圓曲線同源密碼系統的舊一支即 SIKE, 這是仿造 Diffie-Hellman 橢圓曲線金鑰交換,但必需把橢圓曲線上的點當做傳輸的一部份。它的現況是比 CSIDH 要久要快但是沒有 CSIDH 的金鑰和傳輸量那末短。同樣的它的安全性也尚待考驗。

1. 二三事

* NIST 的人向我道歉他說本來應該發信給 GeMSS 和 GUI 的作者群請求合併的，但是他們直到最後還打算兩個一起否決掉 (太慢) 直到最後匆忙決定要留下一個。因為 GUI 一開始的參數挑選有些問題而 GeMSS 的作者沒有犯下什麼錯誤而選了後者。

1. 建議

我們在這次會議吸收了不少新知並和舊友進行了很多討論。我們建議有機會應該能多讓國內學者參與工作坊形式這樣的國際學術活動。